Operational risk and the three lines of defence in UK financial institutions: is three really the magic number?
Mabwe, Kumbirai; Ring, Patrick; Webb, Robert

Published in:
Journal of Operational Risk

DOI:
10.21314/JOP.2017.187

Publication date:
2017

Document Version
Peer reviewed version

Operational risk and the three lines of defence in UK financial institutions: Is three *really* the magic number?

Abstract

There has been growing interest in the need for financial services firms to develop and implement robust systems and structures for managing operational risk. While there now appears to be some consensus in terms of definitions, quantification and modelling, firms are struggling with the qualitative side of operational risk management, particularly in relation to financial institutions' operational risk governance, where the three-lines of defence model has become standardised. At the same time, corporate scandals post-financial crisis continue to indicate deficiencies in operational risk governance. As a result, our paper examines the three lines of defence in the context of operational risk management in UK financial institutions, focusing upon roles and responsibilities and then analyses the effectiveness of the traditional three lines of defence model. We find a lack of common understanding of the lines of defence in financial institutions which is leading to duplication of roles and gaps in coverage. This is concerning for the industry, the economy and regulators.

Key Words: Governance, Operational Risk, Risk Management, Three lines of defence

Introduction

Operational risk is by no means a new phenomenon; nevertheless it is an increasingly significant issue within the financial services industry (Tescher et al, 2008; McCormack and Sheen, 2013). Among the factors attributed to its rise, Sironi and Resti (2007) and Kallenberg (2009) note increased dependency on technology and automation, increasing complexity of new products in financial services globalisation, and regulation and de-regulation of the financial services industry. These factors have created higher degrees of complexity and uncertainty in business operations, making operations and the operating environment riskier; and alongside widely publicised cases adding to significant losses, have led to a renewed interest in operational risk management amongst financial institutions, regulators and academics (Waring, 2001; Helbok and Wagner, 2006; McCormack and Sheen, 2013). In turn, financial institutions have recognised the need to develop more focused and coherent approaches for managing operational risk.

Traditionally, if they defined and managed operational risk at all, financial institutions relied on 'stand-alone' risk managers, control functions, auditors, and insurance, all operating largely independently from each other, to manage operational risk (see Buchelt and Unteregger 2004; Medova and Berg-Yeun, 2009). However, such a 'silo' approach to operational risk management resulted in gaps in analysis, a lack of process to aggregate critical risks, and inadequacies in sharing risk information across organisations. As a result, financial institutions have increasingly come to place reliance on the so called 'three lines of defence' as a model of risk governance (Bontis 2001; Illies et al, 2006).

While any framework for operational risk management and governance should exist within an enterprise risk framework (reflecting the nature, culture and structure of an organisation itself), industry, regulators and academic literature have all promoted the implementation of the three lines of defence governance model (3LOD). Anderson & Daugherty (2012) Basel (2012) Hughes (2011) IIA (2013) and Tescher et al. (2008) all argue that it provides the most effective way to integrate risk governance and communicate risk amongst the various functions involved in operational risk management and control, as well as assigning responsibilities and clarifying roles between the various functions, throughout financial institutions. As a consequence, the 3LOD has been widely adopted and generally accepted as a standard approach by financial institutions (PWC, 2012) as well as having become integral to regulators' approaches to regulating operational risk (BCBS, 2014). The financial services sector is not alone in this approach to operational risk (see COSO 2015) but the 3LOD has been particularly relied upon to ensure operational risks and controls are comprehensively assigned, coordinated, monitored and communicated within financial institutions (FSA 2010; BCBS 2014).

Yet, as the 3LOD approach has developed within financial institutions, it is also clear that they have continued to incur major operational risk losses (de Fontouvelle et al., 2006; BCBS 2009). Whilst these events have influenced developments in operational risk management (Power, 2005; McCormack and Sheen, 2013) the more recent fallout from the LIBOR scandal (Koblenz et al, 2014) indicates that problems may remain in the implementation of the 3LOD to address operational risks. This paper therefore examines the operation of the 3LOD in major UK financial institutions, and in particular draws attention to differences between the 'theory' and 'practice' of the

3LOD model, highlighting differences that may create challenges in managing operational risk. It adds to recent literature by identifying potential difficulties in the how the 3LOD are implemented (see, for example, Ashby et al. 2012 and Power et al., 2013), and provides evidence pointing to ways financial institutions may improve the implementation of the 3LOD and thereby their management of operational risk.

Defining the three lines of defence approach and its variations

Traditionally, the 3LOD found in operational risk management has been based on 'defence in depth', providing safeguards through 'layers' of risk management and risk monitoring (Reason, 1990). A key element of this approach is that each layer, and its accompanying responsibilities and accountabilities, are clearly delineated (Bontis 2000; Illies et al, 2006). The first line consists of business frontline staff who undertake tasks within assigned limits of risk exposure and are responsible and accountable for identifying, assessing and controlling the risks within their business function. In addition, they are responsible for implementing corrective actions to address, process and control deficiencies. Essentially, as outlined by the BCBS (2014) and Chambers (2014), the first line of defence involves day to day risk management at the operational level.

The second line of defence concerns the risk management function, often comprising of the operational risk management (ORM) and compliance functions. The second line of defence's responsibilities includes designing the operational risk management tools to be used by the first line to identify and manage risks. In addition, it applies an 'independent challenge' to the use and output of the operational risk management tools deployed, and develops and maintains policies, standards and guidelines concerning the

management of risk (IIA, 2013; FSA 2012; Chambers, 2014). Bryce et al, (2013) state that the second line of defence monitors the risk policies, appetite and controls which the first line must follow.

The third line of defence, the internal audit function, provides independent assurance that both the first and second lines of defence are operating effectively (McCormack and Sheen, 2013). Internal audit review both the business frontline and the oversight functions to ensure that they are carrying out their tasks to the required level of competency.

In order to ensure the 3LOD framework is operating effectively, executive officers, boards and risk committees receive reports from audit, oversight and the business, enabling them to act on items of concern from any of the three lines (IIA, 2013). However, it remains imperative that the executive also articulates a clear vision of the approach to risk management required across the organisation to achieve its overall objectives; which, in turn, provides the necessary 'tone from the top' to inform the risk management policies, procedures and cultures that must underpin the 3LOD. The BIS (2010) identifies the essential role of executive management, along with the board, in helping to set the correct 'tone at the top': providing oversight of those they manage; ensuring that an institution's activities are consistent with business strategy and that risk tolerances/appetites and policies are approved by the board. As noted by Doughty (2011), the challenge is ensuring that the expectations of senior management and the operational practice of the 3LOD are aligned. When correctly embedded within an enterprise-wide approach to the management of risk, it is argued that the 3LOD can provide a coherent and comprehensive approach to operational risk management,

reducing the frequency and impact of risk events and reflecting the risk culture, appetite and objectives of the organisation. To achieve this, the least that is required is that financial institutions position the board and executive management within, as opposed to separate from, the lines of defence.

However, in practice this ideal has proved culturally and operationally problematic, and there has emerged a number of 'versions' of the 3LOD model (McCormack and Sheen, 2013; Ashby et al, 2012). These versions have tended to extend the lines, or 'layers', of defence to incorporate the executive of an organisation, as well as other stakeholders, within the lines of defence (see Drury, 2009; Deloitte, 2012; Lyons 2015; Protiviti, 2013). For example, Lyons argues that elected board members should be assigned with responsibility for jointly overseeing the activities of the organization and be accountable to the shareholders for the organization's strategy and performance, and so argues (Lyons 2011, 2015) for a clearly established fourth internal line of defence: board committees and sub-committees, and a fifth internal line of defence: the board of directors itself. The fourth line provides "oversight of individual defence activities, such as governance, risk management, and compliance" (2011:5), with the Board being "the last custodians of the internal corporate oversight process" (2011:15). In fact, Lyons (2011) goes further in identifying four further, 'external' lines of defence, incorporating external auditors, shareholders, ratings agencies and regulators.

Although the potential monitoring roles of certain bodies external to financial institutions is well-established; as a matter of practice, if a 'lines of defence' model is to be adopted by banking organisations, then it must inevitably have an internal focus. In this regard, Lyons' position concerning 'internal' lines of defence can be interpreted as

an attempt to more clearly articulate executive management's position in any 'lines of defence' model. Lyons believes that the elected board members should be assigned with responsibility for jointly overseeing the activities of the organization and be accountable to the shareholders for the organization's strategy and performance. So whilst the traditional 3LOD recognises an oversight role for executive management and the board of directors, it might be argued it fails to adequately position and incorporate these roles within a holistic and strategic 'lines of defence' model.

In a slightly different approach to broadening the 3LOD, Protiviti (2013) characterises the first line of defence as the 'tone of the organisation', capturing "the collective impact of the tone at the top, tone in the middle, and tone at the bottom on risk management, compliance and responsible business behaviour" (Protiviti, 2013:2). Broadly speaking, this might be regarded as the risk culture of the organisation (see IRM, 2012). The difficulty with this approach to the lines of defence is that it moves away from using the 3LOD model to identify specific roles and to allocate responsibility for those roles: treating a line of defence as being constituted by one particular characteristic, or state, of an organisations 'tone'.

The issue of how that state is created, and how responsibility for creating it is allocated, is left unanswered. In fact, if that 'state' can be regarded as the risk culture of the organisation, it might be suggested that it involves a complicated and recursive inter-relationship with both the attitudes and behaviours within that organisation (IRM, 2012). This goes well beyond specific roles and responsibilities and so Protiviti's first line of defence is perhaps best regarded as acknowledging the importance of the

environment within which the 3LOD operate to the latter's effectiveness, rather than constituting a line of defence in itself.

Another interesting line of thought draws attention to the effectiveness of the traditional 3LOD arguing that as businesses increase in size and regulatory and risk environments become more complex, the three lines become more blurred or 'fuzzy' (see Ashby et al, 2012; PWC, 2012; Deloitte, 2012; Power et al., 2013). As such, while the 3LOD model, as promulgated by regulators and industry bodies, generally provides a clear operational model with obvious distinctions between each of the three lines, in practice the model is being adapted by institutions to meet the exigencies of coping with an increasingly complex business environment. This can result, for example, in "role tensions and ambiguities at the interface between the first and second line" (Power et al., 2013:29).

Despite these differences in approach, it is clearly recognised that, fundamentally, senior executives and the board of directors collectively have responsibility for establishing an organization's objectives, defining high-level strategies to achieve those objectives, and establishing governance structures to best manage risk (FSA, 2010; BCBS, 2014; COSO, 2015). At the same time, it is also apparent that a 'lines of defence' model, and specifically the 3LOD model, is regarded as the basis of managing risk within financial institutions. It is the operationalization of the 3LOD model in financial institutions, the manner in which the model is being customised to fit financial institution operations, and the challenges this creates, that are the focus of this research.

Methodology and Discussion

The current paper is part of a broader study investigating operational risk governance and internal control frameworks in UK financial institutions since the 2000s. Whilst the population for this study was employees experienced in operational risk management in financial institutions incorporated in the United Kingdom, the selection of the research sample was guided by Basel II's definition of large internationally active financial institutions. These institutions vary from firms where investment banking is the main driver of revenue to others where investment banking is just one of several businesses and does not dominate the overall business agenda or revenue profile of the financial group (Mullin, 2006). Importantly, these institutions are the most influential, and the ones that would have both implemented ORM techniques as required by Basel and most likely adopted what were considered to be good or best practices concerning operational risk in general, and the 3LOD in particular.

The source of data is interviews with operational risk managers, senior financial institution operatives and operational risk consultants working within the financial institutions that are the subject of this study. The interviewees were chosen based on a non-probability judgement basis, which enabled data to be gathered from interviewees encapsulating a wide range of experience and characteristics (Marshall, 1996). In this regard, each participant was chosen in relation to their exposure to, and experience in, operational risk management and governance. In all, twenty five semi-structured interviews were conducted with operational risk managers, operational risk training consultants and operational risk officers in UK financial institutions between May 2013 and April 2014. The data was then transcribed and thematically analysed.

As we have discussed, there has been unrelenting pressure on financial organisations to pay more attention to their operational risk management and governance, particularly in the aftermath of the 2007-2010 financial crises. As a result, when discussing operational risk, 3LOD became a 'catch phrase', frequently used in all interviews and subtleties in approach needed to be teased out. For example, the term was generally used in a manner that assumed a common understanding, and implied a 'taken for grantedness':

> We have the 3 lines of defence like most banks here..... and most of the analysis is made by the first line (Interviewee 24)
>
> There is also growing awareness of the three lines of defence and that we can't leave this (risk management) to other people (Interviewee 02)
>
> Three lines of defence is kind of helpful in getting the idea across that risk needs to be embedded on a day-to-day (Interviewee 08)
>
> In this bank the 3 lines of defence is quite mature it has been around for a long time (Interviewee 19)

The implication and assumption was that the nature and function of the 3LOD was generally agreed and understood across these organisations and, indeed, the industry. However, on further probing, we found, as expected from previous studies (e.g. Power et al., 2013) a need to dig beneath the surface, and the themes that emerged from this analysis are discussed below.

Co-existence of a central risk management function and the three lines of defence model

We found evidence that a majority of financial institutions have adopted the 3LOD model in some shape or form in line with that reported by, amongst others, the FSA (2010) and the BCBS (2014). Interestingly, the majority of interviewees indicated that a centralised operational risk management function has, to a significant extent, been

replaced by the 3LOD model. Meaning that institutions are using the 3LOD model as a foundation on which to build upon:

> In terms of structures I would say it's a combination of central units and it being managed in the business line. Strictly speaking I would say most banks of different sizes have adopted a 3LOD model (interviewee 08).

> The expertise for the risk function was built up in the (central) risk teams and then developed into where we need to build more risk knowledge as in when we had the central unit, but now they have lifted them and put them back into full time business so this has then created the back-up structure, the risk and control structure. (Interviewee 05)

However, it was also clear from the interviews that, for some financial institutions, centralised operational risk management functions still co-existed alongside the first line of defence. This could suggest some financial institutions' operational risk governance processes may still be 'migrating' over to the 3LOD model – which could create issues and missed risk events. This finding is in line with recent evidence from the Basel Committee on Banking Supervision (BCBS) which, on reviewing operational risk practices, found that "many banks also noted that they are still in the process of implementing a more refined approach to assigning specific responsibilities to the three lines of defence" (BCBS, 2014:5) That said, interviewees in this study did not refer to centralised risk management as some kind of transition or temporary situation, but were more likely to refer to it as a 'support and back up structure' (see Interviewee 05 above). It may therefore be argued that, rather than a transition or 'refining' process, some financial institutions may lack confidence, or be unwilling, to allocate day-to-day risk management completely to business functions, and seek comfort in their centralised risk function in support.

This can clearly create problems for institutions and regulators if this situation continued in the more medium to long term – belying the rationale of the 3LOD approach. First, there is a danger that having such a 'belt and braces' approach may result in a lack of clear division between the first and second lines of defence, resulting in the kind of blurring noted in existing literature (Ashby et al, 2012; PWC, 2012; Deloitte, 2012; Power et al., 2013). Second, that lack of clarity can also result in complacency or gaps as a result of dubiety in role responsibilities when it comes to operational risk management. Third, the expected operational efficiencies in resource allocation and communication gained through the implementation of the 3LOD may be diminished. Clearly, regulators need to aware of these issues in order to monitor the effectiveness of operational risk management both within and between institutions.

Model Flexibility, Gaps and Duplication

In the course of the interviews, it became clear that financial institutions were implementing the 3LOD model in a way that suited their size and operating structure, and this seemed to result in differences with regard to exactly how lines of defence (particularly the first and second lines) operated in practice. Such differences should raise alarm bells about the agreed upon nature of the 3LOD model, as more than half of our interviewees claimed there was no clear cut distinction as to where the demarcations between lines of defence are drawn, and exact points of demarcation varied:

> … and where it gets more complicated is in the second line of defence where you often have people whose responsibility it is to exercise oversight over a specific business unit and then you have a group of people who exercise general oversight so obviously if the people who are exercising oversight on a business unit that get drawn too closely to the business unit then they cease to do their main function which is to challenge that business unit (Interviewee 11)

> It is within each individual and business line so if they (first line) can do risk function themselves, we can carry out oversight .... but there should be more clarity as to what they should do and what we should do then we can facilitate that and provide oversight (Interviewee 03).

> The three lines of defence ....Its largely a question of where accountability lies, where ownership lies and I think one of the important aspects of the structure of the way risk is managed is to have that clarity around who is responsible for what (Interviewee 13)

As well as underlining points made previously, these findings suggest that the demarcation of roles between the first and the second line of defence is, indeed, fuzzy (Ashby et al, 2012; PWC, 2012; Deloitte, 2012; Power et al., 2013). A key area of concern was found to be in the second line, with the oversight function becoming more involved with the business line than the traditional 3LOD structure would suggest. As the quotes above indicate, there can be a divergence between theory and practice as the second line eventually 'moves over' to undertake some of the responsibilities of the first line. This creates a gap in the governance framework as the second line loses its 'independent' powers of oversight and challenge. Further, it may create an element of duplication between the first line and the 'moved over' second line. This certainly supports the findings of blurred lines of responsibilities reported by Ashby et al. (2012).

Yet, our research also suggests that, in this blurred and fuzzy space which falls between the lines, there is a varying range of activities that are being undertaken by the second line of defence. In some institutions it appeared the second line undertook the cross consolidating and analysis of data, whilst in others the analysis of data was done by the first line and the second line reviewed the figures. Yet again, in other financial institutions the focus was on providing support to the first line of defence:

> So I am in the second line of defence and we deal very much with cross consolidating the data that we get from the business lines and also for operational risk as a framework or discipline we look at rolling out the RCSA process regularly and event

> management process and also operational risk scenario analysis process and for operational risk ….. I suppose that is it in a nutshell (Interviewee04)
>
> We have the 3 lines of defence here and most of the analysis is made by the first line and we in the second line look at them and review them (Interviewee24)
>
> So in terms of operational risk we provide the framework, measure adherence to policy and the whole structure and it varies with banks so, we use the policies that I have said, the application of guidance and support to support business and we cover challenge and monitoring on a regular basis, be it new products or monthly reporting we are coming through with the challenge (Interviewee05)

Such confusion can lead to problems, suggesting there is a lack of common understanding in institutions concerning the functions and responsibilities of the second line of defence, and indeed of the allocation of responsibilities across the 3LOD more generally. Acknowledging differences in size and operations of different organisations, our evidence may also suggest that the 3LOD is being applied in a more flexible and pragmatic manner, reflecting the operational needs and exigencies of individual organisations. Certainly, when probed, none of the interviewees raised mentioned being unable to provide challenge and oversight as an issue. The apparent flexibility and pragmatism found in our data also supports the finding elsewhere that in some cases the second line has become more of a risk management enabler as opposed to a risk challenger and overseer (Power et al. distinguish between 'Partnership Builders' and 'Partnership Overseers' (Power et al., 2013:40)). Such 'enabling' may stray into areas that some might ascribe to the first line of defence, and the rationale of the model itself suggests this will result in duplication and inefficiency. Just as likely, it may create a challenge to the independence of the second line of defence if those in the second line must challenge the work they have contributed to in the first line of defence.

The sub-lines within the 3LOD

Our findings as reported so far suggest that, in an attempt to cope with the inevitable business and organisational complexity of managing risk, financial institutions have adopted a flexible approach to the implementation of the 3LOD which, in turn, has led to blurring of lines. Yet our evidence, and existing literature, also suggests that this flexibility has resulted in the nascent development of different roles *within* the 3LOD structure. In order to move beyond the notion of 'blurring' of the lines of defence, and at the same time retain the potential of the 3LOD as a comprehensive model, it is necessary to begin to sketch out how attempts to develop the 3LOD, and particularly the relationship between the first and second lines of defence, may be understood in the context of the model itself.

One of the themes that emerged from our study is that although it is still regarded as the 3LOD, the approach has been adapted as institutions have latently evolved more than the standard three lines of defence:

> So for me the key is 3LODs, I have seen 7LODs I have certainly seen 5 where it gets complicated is of course for a lot of business units they have embedded operational risk offices in the business units so you end up have a 1a, 1b and 1b being the embedded office ….. (Interviewee11)

> A number of financial institutions do I think introduce an additional layer… line so there is I suppose you could call that a level 1a which sits between levels one and two(Interviewee14)

This development should be distinguished from the earlier discussion of Lyons (2011) Protiviti (2013), since the results of the interviews suggest that these additional lines have evolved within the model, rather than expanded the scope of the model. The suffixes ('a', 'b') indicate these layers exist within, or between, the original lines –

specifically within or between the first and second lines of defence. The use of the suffixes by the interviewees (as opposed to calling them lines 4 or 5) may also suggest they should not be given the same prominence as the original 3LOD; they are 'sub-lines' of defence.

Having established the existence of the sub-lines of defence we now go on to examine the characteristics of these sub-lines in more detail.

Characteristics of the sub-lines of defence

It might have been logical to expect the additional sub-lines to be in the second line of defence – mainly due to the range of the activities that are expected in this line – for example in many cases we found that this line was doing the work that should have been absorbed into the first line of defence. However, our interviewees consistently referred to sub-lines 1a and 1b and it became difficult to discern a consensus around a clear and unambiguous purpose for these sub-lines. Most interviewees differed on the purposes the sub-lines served – suggesting learning by doing approach and that institutions may well still be operating in a more 'siloed' way than chief executives and boards would like to admit. We found that the sub-lines are addressing the practical complexities that full implementation of the 3LOD approach creates for an institution. In some cases, it also appeared the sub-lines were acting as 'comfort blankets' which should make it difficult for any poor risk management to slip through. Interestingly, two particular themes emerged:

i) Sub-lines between first line and second line co-ordinating the first line and the second line:

> A number of financial institutions do, I think, introduce an additional layer which is sort of a risk co-ordination role, which sits within the first line, within the business reporting to the first line and does functional reporting to, and across, the second line so there is, I suppose you could call that a level 1a, which sits between levels one and two that's quite common and helpful I think, as it kind of bridges the gap between the business and the specialist function (Interviewee 14)

ii) Sub-lines within the first line of defence as an embedded oversight risk function:

> The 1a piece of the first line of defence, the people that are doing the business must always own the risk..... and 1b being the embedded oversight office ...they facilitate the development of the framework of operational risk in the business units but they must never own the risk (Interviewee11)

> We do have risk people in the various business lines but there is a dedicated team that forms like an oversight... maybe that is 1b The risks are owned by the business lines which is 1a if I can put it that way and the 1b risk team is there to kind of support, make reviews etc. (Interviewee04)

The co-ordinating role may be understood as a means of helping ensure the effectiveness of the 'partnership' approach between the first and second line, as identified by Power et al. (2013). Here, the sub-line sits within the first line of defence with the purpose of ensuring the second line receives appropriate, adequate and timely risk information from the first line. This avoids the 'blurring' that arises when the second line ends up having to collect the data that they are then supposed to 'police and challenge.'

By contrast, the embedded risk function goes further in embedding a business/supervisory operational risk function within the first line of defence. On the one hand, this approach may be a response to limits identified in the development of risk management expertise amongst first line business staff or to a need for more resources (BSBS, 2014:36). In this scenario, risk management expertise resides in the first line of defence, but specifically in staff who are distinguished, by that expertise,

from front line business staff (hence 1b). Specifically identifying this role as 1(b) may create greater clarity, avoiding the 'blurring' that may arise where the second line of defence becomes involved in the identification and assessment of risk and controls (the role of the first line of defence under the traditional 3LOD).

On the other hand, the development of these sub-lines may also be an understandable response by senior managers to the prospect of review by the second line of defence – undertaking their own 'pre-review' review to ensure that no significant issues are likely to be raised when the second line subsequently reviews the business unit. A majority of interviewees indicated that 1a is the business line and 1b undertakes risk controls and therefore is the embedded risk oversight function. Upon probing, we found that 1a is checked by 1b, with the second line providing oversight. What remains unclear is whether the second line is providing oversight to both 1a and 1b, or just one of them. Either there is a duplication of risk oversight, or the possibility of a lack of oversight if the second line of defence places any reliance on the work of line 1b. The possibility also exists for disagreement as a result of differences in the separate supervisory oversight outcomes of lines 1b and 2.

Significantly, in terms of overall operational risk management and the avoidance of risk events, the majority of the interviewees believed the additional lines were bridging gaps and improving risk coordination and reporting. However, a minority of the interviewees believed that sub-lines may create misunderstanding as to roles and responsibilities, and may well create more gaps. This is illustrated by another interviewee who commented:

> So for me the key is 3LODs, I have seen 7LODs I have certainly seen 5 but once you break it down beyond those 3 then there is room for people to misunderstand their roles and responsibilities so in terms of roles and responsibilities and organisational layout I like to see some framework adopted (Interviewee 11)

What is apparent is the rather ad hoc nature of the approaches across our interviewees' institutions. That said, whilst the need for other sub-lines is identified by some interviewees, this last extract suggests that rather than discussing 'lines' it may be more productive to frame the discussion in terms of the additional roles and functions being undertaken; for example, the 'co-ordinating' and 'embedded risk oversight' functions identified above. Thereafter, the key task becomes one of structuring the additional identified roles and functions within the 3LOD in such a way as to cover the gaps and resolve the risk management issues that arise in running a complex business, whilst at the same time retaining the core structure and purpose of the 3LOD. This retains an organisation's ability to undertake the three core functions of operational risk management, challenge and independent review at the heart of the 3LOD, but to do so within a flexible framework which facilitates the organisation's own risk culture and an enterprise-wide approach to risk management. It must be noted, however, that there is no single approach across the sector and while such flexibility may be a strength, it may also lead to further issues regarding the capture and management of risk events.

It should also be noted that the BCBS (2014), in discussing how more complex financial institutions are refining their approach to operational risk management, has identified lines 1a and 1b as well as 2a and 2b within the 3LOD (2014:34). Their analysis is based on the examination of evidence from a wide range of financial institutions. However, there is a danger that the same issues experienced with the 3LOD and discussed in this analysis, will be replicated by this 'enhanced' three lines of defence. The primary issue

should be effective risk management, not the ability of an organisation to evidence a framework with three distinct levels, or further 'enhanced' sub-levels, to a regulator or other interested parties. To that extent, and within the broad framework and rationale of the 3LOD, the most important issue must be the clear identification of the risk management roles and functions within an organisation. That done, lines of communication, removal of gaps and overlap, and ensuring the availability of necessary skills, can be established and embedded. The identification of the sub-lines 1a and 1b, and their role and function, may be a useful contribution to this task; however, they should not act as an inhibitor to financial institutions refining their approach to the adoption of the 3LOD in operational risk management.

Discussion and Conclusion

Our study focuses upon the three lines of defence risk governance model which has been widely adopted and generally accepted as a standard approach by financial institution management and regulators. We find that there is no single common understanding of the 3LOD in UK institutions and that there is a range of practices with regard to implementation of the model – blurring the lines of the model. We do find that the 3LOD has been adopted by financial institutions as their *de facto* model for operational risk management, but there is divergence between theory and practice. That said, for organisations where there is clear segregation of duties and well defined responsibilities, the 3LOD may simply put a name to the existing structure. Even where this is not the case, as in the case of most large financial institutions, attempting to adopt the 3LOD encourages risk practitioners, and their organisations more generally, to consider how they should organise and deliver operational risk management, and

provides a foundation for discussion within and across organisations. Siloes, however, remain.

Our study reports several themes arising in relation to the way financial institutions have organised themselves in implementing the 3LOD approach. First, our research confirms the 'blurring' identified by Ashby et al. (2012). There was evidence of the second line becoming involved in tasks that, according to the model, one would expect to be undertaken in the first line. This sometimes appeared to be a response to the need to acquire the data necessary to undertake their second line supervisory role, perhaps as a result of lack of resources or skills to undertake this task in the first line. At the same time, there was also evidence of a nascent risk supervision function being carried out in the first line of defence. We suggest this may be due to a desire amongst senior managers of business units to be satisfied that, when it comes to meeting the challenges of the second line of defence, their unit will perform well.

Second, we found that this blurring has led to the development of sub-lines of defence. These sub-lines were highlighted by a majority of interviewees, all pointing to what they regarded as an embedded risk function within the first line of defence. It was clear that a key driver in this development was to provide more efficient co-ordination and communication between the first and second lines of defence by having clearly identifiable risk management expertise within the first line of defence. A majority of interviewees indicated that 1a is the business line and 1b undertakes risk controls and therefore is the embedded risk function. Upon probing, we also found that alternatively the risk controls exercised by 1a may be 'checked' by 1b with the second line providing oversight.

It seems then that sub-lines 1a and 1b are developing as a means of identifying and enhancing risk expertise in the first line of defence, and in particular in relation to risk supervisory and communication capacity. What remains unclear is whether the second line of defence is providing oversight to both 1a *and* 1b, or 1a or 1b only; what amount of duplication exists between 1b and the second line; and whether this approach may create gaps in supervision or challenges to risk management in the front line of the business. Relations between line 1b and the second line of defence may also give rise to questions of whether the second line can remain independent.

What is clear is that there remains a danger that the unique benefits of creating an integrated approach to operational risk management could be lost as a result of gaps or duplications leading to the loss of a clear and unambiguous separation and co-ordination of roles and responsibilities. Practically there may be sub-lines which are not formally recognised as defending anything, yet informally play a significant part in the 3LOD structure. This could indicate flaws in formal governance structures, leading to a failure to provide comprehensive defence coverage for financial institutions.

These findings also raise some important practical issues for financial institutions. While the 3LOD may be seen as a flexible model within which they can negotiate around the edges, the evidence of increasing prevalence of lines 1a and 1b suggests financial institutions may need to formally revise the structure of their 3LOD framework to improve clarity of responsibility for operational risk management. Equally, the existence of lines 1a and 1b may indicate a need for financial institutions to consider existing skill sets concerning the management of risk within the business, and within the 3LOD in particular. This might involve more risk management training in the

first line of defence so as to enable the 3LOD to operate as it is classically understood. Alternatively, if this classical separation is not possible, or not desirable or practical in specific business contexts, then there may need to be an assessment of the skill sets needed for roles that might be typical of 1a or 1b in a specific organisation. At the same time, the existence of these sub-lines may suggest a career progression path, from 1a to 1b and then line 2, that needs to be understood and managed.

When it comes to understanding the 3LOD in the sector, this research illustrates again the all too common mis-match between the theory and how it is generally assumed to be applied in organisations, and the variations in its practical implementation as financial institutions cope with the exigencies of their business. The response must be to abandon lazy assumptions concerning the 3LOD. When it comes to managing operational risk, the best practice will come from those financial institutions who understand how their lines of defence work in practice, and manage them accordingly.

References

Anderson, U., and Daugherty, B., (2012): The third line of defence: Internal audit's role in the governance process, Internal Auditing 26, no. 4 38–41.

Ashby, S., Palermo, T. and Power, M. (2012). Risk culture in financial organisations - An interim report, CARR discussion paper (November), 1-25

BCBS (2009). *Results from the 2008 Loss Data Collection Exercise for Operational Risk.* Bank for International Settlements BCBS (2012), ''Core principles for effective banking supervision'' September 2012 Bank for International Settlements,

BCBS (2014), ''Review of the Principles for the Sound Management of Operational Risk'' October 2014 Bank for International Settlements,

BIS (2010), ''Principles for enhancing corporate governance'' October *2010 Bank for International Settlements.*

Bontis, N. (2001). Assessing knowledge assets: a review of the models used to measure intellectual capital. International journal of management reviews, 3(1), 41-60.

Bryce, C., Cheevers, C., & Webb, R. (2013). Operational risk escalation: An empirical analysis of UK call centres. International Review of Financial Analysis, 30, 298-307.

Buchelt, R. and Unteregger, S. (2004). Cultural risk and risk culture: operational risk after Basel II. Financial Stability Report 6. http://www.oenb.at/en/img/fsr_06_cultural_risk_tcm16-9495.pdf.

Chambers, A., (2014) Goodheart's Law? The Third line of defence: Second Thoughts Part II Internal Auditing

COSO (2015) Leveraging coso across the three lines of defence http://www.coso.org/documents/COSO-2015-3LOD-PDF.pdf (Accessed 21April 2016)

De Fontnouvelle, P., DeJesus-Rueff, V., Jordan, J. S., & Rosengren, E. S. (2006). Capital and risk: New evidence on implications of large operational losses. *Journal of Money, Credit and Banking*, 1819-1846.

Deloitte (2012) 3D blurred version the new paradigm of three lines of assurance Available on http://www.iia.org.au/sf_docs/default-source/sopac-previous-confs/SOPAC_2012_3D_Presentation.pdf?sfvrsn=0 (Accessed 22 April 2015)

Doughty., K. (2011) the Three Lines of Defence Related to Risk Governance SACA JOURNAL VOLUME 5, 2011

Drury, N., (2009) why has operational risk returned to the limelight? the market magazine – Winter 2009 Available on http://content.markitcdn.com/corporate/Company/Files/MagazineEntireIssue?CMSID=a53435805783415a89a881c53af7afae (Accessed 22 April 2015)

Financial Services Authority (2010) "Assessing Possible Sources of Systemic Risk from risk from hedge funds Available at : http://www.fsa.gov.uk/pubs/other/hf_survey.pdf[accessed 12th April, 2013]

Financial Services Authority (FSA). 2012a. Risks to Consumers from Financial Incentives: GC 12/11, Guidance Consultation. London: Financial Services Authority.

Helbok, G., & Wagner, C. (2006). Determinants of operational risk reporting in the banking industry. *Available at SSRN 425720*.

Hughes, P., (2011) Bank internal audit…Third line of defence or first line of attack? Risk Reward Risk Update (January 2011). Available at: http://www.riskre-wardlimited.com/admin/pdf/RU%20Jan%202011%20PH-Internal%20Audit.pdf (accessed Aug 11, 2013).

IIA (2013) The Three Lines of Defence in Effective Risk Management and Control, The Institute of Internal Auditors (January 2013), [Online], Available: http://na.theiia.org (accessed 19April 2014)

Ilies, R., Scott, B. A., & Judge, T. A. (2006). The interactive effects of personal traits and experienced states on intra individual patterns of citizenship behaviour. Academy of Management Journal, 49(3), 561-575.

Institute of Risk Management (IRM) (2012) Risk culture: Guidance from the Institute of Risk Management. London: Institute of Risk Management.

Kallenberg, K. (2009). Operational Risk Management In Swedish Industry: Emergence Of A New Risk Paradigm. *Risk Management*, *11*(2), 90-110.

Koblenz, M. R., Labbate, K. M., & Turner, C. C. (2014). LIBOR: Everything You Ever Wanted to Know But Were Afraid to Ask. *The Journal of Business, Entrepreneurship & the Law*, *6*(2), 4.

Lyons, S. (2011). Corporate oversight and stakeholder lines of defence. In The Conference Board Executive Action Report (No. 365).

Lyons, S. (2015) Enterprise Risk Management and the Five Lines of Corporate Defence The Journal of Enterprise Risk Management Vol (1), No 1 pp 56-81

Marshall, M. N. (1996). Sampling for qualitative research. Family practice, 13(6), 522-526.

McCormack, P., & Sheen, A. (2013). Operational risk: Back on the agenda. *Journal of Risk Management in Financial Institutions*, *6*(4), 366-386.

Medova, E. A., & Berg-Yuen, P. E. (2009). Banking capital and operational risks: comparative analysis of regulatory approaches for a bank. Journal of financial transformation, 26(7) pp 12-23.